On the irreducibility of multivariate subresultants

Sur l'irréductibilité des sous-résultants multivariés

Laurent Busé [a] Carlos D' Andrea [b]

[a] *INRIA, GALAAD, 2004 route des Lucioles, B.P. 93, 06902 Sophia-Antipolis cedex, France. Tél: +33-(0)4-92-38-76-51, fax: +33-(0)4-92-38-79-78.*

[b] *Department of Mathematics UC Berkeley & The Miller Institute for Basic Research in Science. 1089 Evans Hall, Berkeley, CA 94720-3840 USA. Tél: +1-(510)-642-6947, fax: +1-(510)-642-8204.*

Abstract

Let $P_1, \ldots, P_n$ be generic homogeneous polynomials in n variables of degrees $d_1, \ldots, d_n$ respectively. We prove that if ν is an integer satisfying $\sum_{i=1}^n d_i - n + 1 - \min\{d_i\} < \nu$, then all multivariate subresultants associated to the family $P_1, \ldots, P_n$ in degree ν are irreducible. We show that the lower bound is sharp. As a byproduct, we get a formula for computing the residual resultant of $\binom{\rho-\nu+n-1}{n-1}$ smooth isolated points in $\mathbb{P}^{n-1}$.

Résumé

Soient $P_1, \ldots, P_n$ des polynômes homogènes génériques en n variables de degré respectif $d_1, \ldots, d_n$. Nous montrons que si ν est un entier tel que $\sum_{i=1}^n d_i - n + 1 - \min\{d_i\} < \nu$, tous les sous-résultants multivariés de degré ν des polynômes $P_1, \ldots, P_n$ sont irréductibles. Nous montrons également que cette borne est atteinte dans des cas particuliers. Comme conséquence directe nous obtenons une nouvelle formule pour le calcul du résultant résiduel de $\binom{\rho-\nu+n-1}{n-1}$ points lisses isolés dans $\mathbb{P}^{n-1}$.

Classical subresultants of two univariate polynomials have been studied by Sylvester in the foundational work [13]. Multivariate subresultants, introduced in [2], provide a criterion for over-constrained polynomial systems to have Hilbert function of prescribed value, generalizing the classical case. To be more precise, let $\mathbb{K}$ be a field. If $P_1, \ldots, P_s$ are homogeneous polynomials in $\mathbb{K}[X_1, \ldots, X_n]$ with $d_i = \deg(P_i)$ and $s \leq n$, $H_{d_1,\ldots,d_s}(.)$ is the Hilbert function of a complete intersection given by s homogeneous polynomials in n variables of degrees $d_1, \ldots, d_s$, and S is a set of $H_{d_1,\ldots,d_s}(\nu)$ monomials of degree ν, the subresultant Δ_S^ν is a polynomial in the coefficients of the $P_i's$ of degree $H_{d_1,\ldots,d_{i-1},d_{i+1},\ldots,d_n}(\nu - d_i)$ in the coefficients of P_i $(i = 1, \ldots, s)$ having the following universal property: $\Delta_S^\nu \neq 0$ if and only if $I_\nu + \mathbb{K}\langle S\rangle = \mathbb{K}[X_1, \ldots, X_n]_\nu$, where I_ν is the degree ν part of the ideal generated by the P_i's (see [2]).

Multivariate subresultants have been used in computational algebra for polynomial system solving ([10],[14]) as well as for providing explicit formulas for the representation of rational functions ([11,6,7,12]).

Email addresses: `lbuse@sophia.inria.fr` (Laurent Busé), `cdandrea@math.berkeley.edu` (Carlos D' Andrea).

The study of their properties is an active area of research ([3,4,6,7,8]). In particular, it is important to know which S verify $\Delta_S^\nu \neq 0$, and which of these Δ_S^ν are irreducible (see the final remarks and open questions in [2] and the conjectures in [7]). Partial results have been obtained in this direction. In [5] it is shown that, if $s = n$ and $\sum_{i=1}^n d_i - n - \min\{d_i\} < \nu$, then for every set S of monomials of degree ν and cardinal $H_{d_1,\dots,d_n}(\nu)$, the polynomial Δ_S^ν is not identically zero. Moreover, in [4], it is also proved that if $s = n$, $\nu = \sum_{i=1}^n d_i - n$, and $S = \{x_j^\nu\}$ for $j = 1,\dots,n$, then Δ_S^ν is an irreducible polynomial in the coefficients of the $P_i's$. In [8, Lemma 4.2] the irreducibility of Δ_S^ν is shown for $s = n = 2$, $\max\{d_1, d_2\} \leq \nu$, and $S = \{X_2^\nu, X_1X_2^{\nu-1}, \dots, X_1^{H_{d_1,d_2}(\nu)-1}X_2^{\nu-H_{d_1,d_2}(\nu)+1}\}$.

In this note we study the irreducibility problem in the case $s = n$. Let us introduce some notations in order to state our result. Let $\rho := \sum_{i=1}^n (d_i - 1)$. For $i = 1,\dots,n$ and $\alpha \in \mathbb{Z}^n_{\geq 0}$ such that $|\alpha| = d_i$, introduce a new variable $c_{i,\alpha}$. Let $\mathbb{A} := \mathbb{Z}[c_{i,\alpha}, i = 1,\dots,n, |\alpha| = d_i]$ and set

$$P_i(x_1,\dots,x_n) := \sum_{|\alpha|=d_i} c_{i,\alpha}x^\alpha. \tag{1}$$

Theorem *For every ν such that $\rho - \min\{d_i\} + 1 < \nu$ and every set S of monomials of degree ν and cardinality $H_{d_1,\dots,d_n}(\nu)$, the subresultant $\Delta_S^\nu(P_1,\dots,P_n)$ is irreducible in $\mathbb{A}$.*

Observe that, if $n = 2$, then $\rho - \min\{d_i\} + 1 = d_1 + d_2 - 2 - \min\{d_i\} + 1 = \max\{d_i\} - 1$, and this is equivalent to $\max\{d_i\} \leq \nu$, so our result contains those in [8].

Proof of the Theorem: For simplicity we assume hereafter that $d_1 \geq \ldots \geq d_n \geq 1$. First observe that if $\nu > \rho$ then Δ_S^ν is simply a resultant, and is hence known to be irreducible. So, we can suppose w.l.o.g. that $d_n > 1$. We thus only have to consider integers ν such that

$$\rho \geq \nu > \rho - d_n + 1 = \sum_{i=1}^{n-1}(d_i - 1), \tag{2}$$

where we recall that $\rho = \sum_{i=1}^n (d_i - 1)$. We begin by computing the multi-degree of the subresultants Δ_S^ν; we know (see [2]) that

$$\deg_{P_i}(\Delta_S^\nu) = H_{d_1,\dots,d_{i-1},d_{i+1},\dots,d_n}(\nu - d_i).$$

But from the standard short exact sequence

$$0 \to \frac{R}{(f_1,\dots,f_{i-1},f_{i+1},\dots,f_n)}(-d_i) \xrightarrow{\times f_i} \frac{R}{(f_1,\dots,f_{i-1},f_{i+1},\dots,f_{n-1})} \to \frac{R}{(f_1,\dots,f_n)} \to 0,$$

where $f_1,\dots,f_n$ are homogeneous polynomials of respective degree d_i in a graded polynomial ring R and $f_1,\dots,f_n$ is a complete intersection in R, we deduce

$$H_{d_1,\dots,d_{i-1},d_{i+1},\dots,d_n}(t - d_i) = H_{d_1,\dots,d_{i-1},d_{i+1},\dots,d_n}(t) - H_{d_1,\dots,d_n}(t)$$

for all integer t. It follows that for all integer $\nu \geq \rho - d_n + 1$,

$$\deg_{P_i}(\Delta_S^\nu) = \frac{d_1\ldots d_n}{d_i} - H_{d_1,\dots,d_n}(\nu) = \frac{d_1\ldots d_n}{d_i} - \binom{\rho - \nu + n - 1}{n-1}, \tag{3}$$

where that last equality comes from the facts that $H_{d_1,\dots,d_n}(\rho - t) = H_{d_1,\dots,d_n}(t)$ for all integer t, and $H_{d_1,\dots,d_n}(t) = \binom{t+n-1}{n-1}$ for all $0 \leq t < d_n$. We define $\mathbf{a} := \binom{\rho-\nu+n-1}{n-1}$. As $\mathbf{a}$ does not depend on $i \in \{1,\dots,n\}$ and residual (or reduced) resultants of $\mathbf{a}$ isolated points in $\mathbb{P}^{n-1}$ have the same degree in the coefficients of P_i as the right hand side of (3), this suggest that we compare Δ_S^ν with residual resultants.

We will work with an ideal G defining $\mathbf{a}$ points in $\mathbb{P}^{n-1}$ which is generated in degree at most d_n and such that $G_{d_n-1} \neq 0$. Ideals defining $\mathbf{a}$ points in sufficiently generic position are generated in degree exactly $\rho - \nu + 1$ (see [9, Proposition 4]). Since by (2) we have $d_n > \rho - \nu + 1$, we thus choose such an

ideal $G = (g_1, \ldots, g_m)$, where $\deg(g_i) = \rho - \nu + 1$ for all $i = 1, \ldots, m$, defining $\mathbf{a}$ points in generic position (see [9] for the definition of "generic position"), and hence locally a complete intersection.

Now consider the following specialization of polynomials P_i's

$$P_i \mapsto \overline{P}_i := \sum_{j=1}^{m} p_{ij}(x) g_j(x), \qquad (4)$$

where $p_{ij}(x) = \sum_{|\alpha|=d_i-\rho+\nu-1} c_{ij}^{|\alpha|} x^\alpha$ is a generic polynomial of degree $d_i - \rho + \nu - 1$. There exists a resultant associated to the system $\overline{P}_1, \ldots, \overline{P}_n$, called the *residual resultant*. We denote it by $\mathrm{Res}_G(\overline{P}_1, \ldots, \overline{P}_n)$. Let us recall its main properties (see [1] §3.1).

– $\mathrm{Res}_G(\overline{P}_1, \ldots, \overline{P}_n)$ is a homogeneous and *irreducible* polynomial in the ring of all the coefficients $\mathbb{Q}[c_{ij}^{|\alpha|}]$,

– For any given specialization of the coefficients $c_{ij}^{|\alpha|}$'s sending $\overline{P}_i$ to Q_i, we have

$$\mathrm{Res}_G(Q_1, \ldots, Q_n) = 0 \text{ if and only if } (Q_1, \ldots, Q_n)^{sat} \subsetneq G = G^{sat},$$

– $\mathrm{Res}_G(\overline{P}_1, \ldots, \overline{P}_n)$ is multi-homogeneous: it is homogeneous in the coefficients of each polynomials $\overline{P}_i$, $i = 1, \ldots, n$, and we have

$$\deg_{\overline{P}_i}(\mathrm{Res}_G(\overline{P}_1, \ldots, \overline{P}_n)) = \frac{d_1 \ldots d_n}{d_i} - \mathbf{a}.$$

We are now going to compare this residual resultant with the specialized subresultant $\Delta_S^\nu(\overline{P}_1, \ldots, \overline{P}_n)$, which is non-zero as proved in [4]. We claim that we have the following implications:

$$\Delta_S^\nu(Q_1, \ldots, Q_n) \neq 0 \Rightarrow H_{(\underline{Q})}(\nu) = \mathbf{a} \Rightarrow H_{(\underline{Q})}(t) = \mathbf{a} \text{ for all } t \geq \nu \Rightarrow \mathrm{Res}_G(Q_1, \ldots, Q_n) \neq 0, \qquad (5)$$

where $H_{(\underline{Q})}(.)$ denotes the Hilbert function associated to the ideal $(Q_1, \ldots, Q_n)$. Only the second implication needs to be proved, the others follow directly from the algebraic properties of resultants and subresultants. We know that $H_G(t) = \mathbf{a}$ for all $t \geq \rho - \nu + 1$ (see [9]), and since we have supposed (2), it is a straightforward computation to show that $\nu \geq \rho - \nu + 1$. It follows that, by hypothesis, the ideals G and $(\underline{Q})$ coincide in degree ν and have Hilbert function $\mathbf{a}$ in this degree. As they are both generated in degree at most ν this implies that they coincide in all higher degrees, and therefore they both have Hilbert function equal to $\mathbf{a}$ in these degrees, because G is the defining ideal of a set of points.

Due to (5) and the irreducibility of the residual resultant, we deduce that $\mathrm{Res}_G(\overline{P}_1, \ldots, \overline{P}_n)$ divides $\Delta_S^\nu(\overline{P}_1, \ldots, \overline{P}_n)$. But both polynomials have the same degree, so they must be equal up to a rational number (giving a new formula for computing this residual resultant using [3]). Since this residual resultant is irreducible, and since Δ_S^ν and $\Delta_S^\nu(\overline{P}_1, \ldots, \overline{P}_n)$ have the same multi-degree, this shows that Δ_S^ν is irreducible in $\mathbb{Q}[\mathrm{coeff}(P_i)]$.

It remains to prove that Δ_S^ν is irreducible in $\mathbb{Z}[\mathrm{coeff}(P_i)]$. As it is irreducible in $\mathbb{Q}[\mathrm{coeff}(P_i)]$, we only have to show that Δ_S^ν has content ± 1. Suppose that this is not the case, and let $p \in \mathbb{Z}$ be a prime dividing the content of Δ_S^ν. Let k be the algebraic closure of $\mathbb{Z}_p$. This implies that $\Delta_S^\nu = 0$ in $K := k(\mathrm{coeff}(P_i))$, and hence S is linearly dependent in $K[x_1, \ldots, x_n]/\langle P_1, \ldots, P_n \rangle$, contradicting the main result of [4].

Reducibility in lower degrees: We now exhibit some sets S of degree $\nu = \rho - \min\{d_i\} + 1$ such that Δ_S^ν factorizes. This shows that the lower bound in our theorem is sharp.

- $\mathbf{n = 2}$, $\mathbf{d_1 > d_2}$**:** In this case, $\nu = d_1 - 1 \geq d_2$, and $H_{d_1,d_2}(\nu) = d_2$. Thus Δ_S^ν can be here computed with Sylvester type matrices [13]. However, setting $f_2 = c_0 x_1^{d_2} + c_1 x_1^{d_2-1} x_2 + \cdots + c_{d_2} x_2^{d_2}$, the universal property of the subresultant Δ_S^ν shows immediatly that it is a power of c_0, and we have already seen that its degree is $d_1 - d_2 + 1$; it follows that $\Delta_S^\nu = c_0^{d_1-d_2+1}$, so it can not be irreducible.

- $\mathbf{n > 2,\ d_1 - 1 > d_2 = d_3 = \ldots = d_n = 1}$**:** Again in this case, $\nu = d_1 - 1$ and $H_{d_1,d_2}(\nu) = 1$. Choose $S = \{x_1^\nu\}$ and, if $f_i = c_{1i}x_1 + \ldots + c_{ni}x_n$, $i = 2, \ldots, n$, we set $\delta := \det (c_{ij})_{2\leq i,j\leq n}$. Applying Lemma 4.4 in [6] to this situation, we get that $\Delta_S^\nu = \delta^\nu$. So, Δ_S^ν is not irreducible.

Acknowledgements: This work started during the special year (2002–2003) on "Commutative Algebra" at the Mathematical Sciences Research Institute (MSRI Berkeley). We wish to thank MSRI for its hospitality and for the wonderful working atmosphere it provided. We are also grateful to David Cox, Gabriela Jeronimo and Bernd Sturmfels for their helpful comments on preliminary versions of this paper, and to the anonymous referee for useful remarks improving the presentation of this work.

References

[1] Busé, L. *Étude du résultant sur une variété algébrique.* Ph.D. Thesis, Université de Nice, 2001.

[2] Chardin, Marc. *Multivariate subresultants.* J. Pure Appl. Algebra 101 (1995), no. 2, 129–138.

[3] Chardin, Marc. *Formules à la Macaulay pour les sous-résultants en plusieurs variables.* C. R. Acad. Sci. Paris Sér. I Math. 319 (1994), no. 5, 433–436.

[4] Chardin, Marc. *Formules à la Macaulay pour les sous-résultants en plusieurs variables et application au calcul d'un résultant réduit.* Preprint (extended version of the previous article). Available at `http://www.math.jussieu.fr/~ chardin/textes.html`

[5] Chardin, Marc. *Sur l'indépendance linéaire de certains monômes modulo des polynômes génériques.* C. R. Acad. Sci. Paris Sér. I Math. 319 (1994), no. 10, 1033–1036.

[6] D'Andrea, Carlos; Jeronimo, Gabriela. *Subresultants and Generic Monomial bases.* Preprint 2003.

[7] D'Andrea, Carlos; Khetan, Amit. *Macaulay style formulas for toric residues.* Preprint 2003.

[8] El Kahoui, M'hammed. *An elementary approach to subresultants theory.* J. Symbolic Comput. 35 (2003), no. 3, 281–292.

[9] Geramita, A. V.; Orecchia, F. *Minimally generating ideals defining certain tangent cones.* J. Algebra 78 (1982), no. 1, 36–57.

[10] González-Vega, Laureano. *Determinantal formulae for the solution set of zero-dimensional ideals.* J. Pure Appl. Algebra 76 (1991), no. 1, 57–80.

[11] Jouanolou, J. P. *Formes d'inertie et résultant: un formulaire.* Adv. Math. 126 (1997), no. 2, 119–250.

[12] Mulders, Thom. *A note on subresultants and the Lazard/Rioboo/Trager formula in rational function integration.* J. Symbolic Comput. 24 (1997), no. 1, 45–50.

[13] Sylvester, Joseph H. *A Theory of syzygetic relations of two rational integral functions, comprising an application to the theory of sturm's functions, and that of the greatest algebraic common measure.* Philosophical Transl, 143 (1853) 407–548.

[14] Szanto, Agnes. *Solving over-determined systems by subresultant methods.* J. Symbolic Comput. To appear.